UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

ANTON PERAIRE-BUENO, and
JAMES PERAIRE-BUENO,

Defendants.

SEALED INDICTMENT

24 Cr. ____

24 CRIM 293

COUNT ONE
(Conspiracy to Commit Wire Fraud)

Overview

1. ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO, the defendants, are brothers who studied mathematics and computer science at one of the most prestigious universities in the country. Using the specialized skills developed during their education, as well as their expertise in cryptocurrency trading, ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO exploited the very integrity of the Ethereum blockchain in order to fraudulently obtain approximately $25 million worth of cryptocurrency from victim cryptocurrency traders (the "Exploit"). Through the Exploit, which is believed to be the very first of its kind, ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO manipulated and tampered with the process and protocols by which transactions are validated and added to the Ethereum blockchain. In doing so, they fraudulently gained access to pending private transactions and used that access to alter certain transactions and obtain their victims' cryptocurrency. Once the defendants stole their victims' cryptocurrency, they rejected requests to return the stolen cryptocurrency and took numerous steps to hide their ill-gotten gains.

2. ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO, the defendants, meticulously planned the Exploit over the course of several months. Among other things, they learned the trading behaviors of the victim traders whose cryptocurrency they ultimately stole. As they planned the Exploit, they also took numerous steps to conceal their identities and lay the groundwork to conceal the stolen proceeds, including by setting up shell companies and using multiple private cryptocurrency addresses and foreign cryptocurrency exchanges. After the Exploit, the defendants transferred the stolen cryptocurrency through a series of transactions designed to conceal the source and ownership of the stolen funds.

3. Throughout the planning, execution, and aftermath of the Exploit, ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO, the defendants, also searched online for information about, among other things, how to carry out the Exploit, ways to conceal their involvement in the Exploit, cryptocurrency exchanges with limited "know your customer" procedures that they could use to launder their criminal proceeds, attorneys with expertise in cryptocurrency cases, extradition procedures, and the very crimes charged in this Indictment.

Background on Cryptocurrency, the Ethereum Network, and Maximal Extractable Value

4. Cryptocurrency is a digital currency in which transactions are verified, and records are maintained, by a decentralized system using cryptography. Like traditional fiat currency, there are multiple types of cryptocurrency. Cryptocurrency owners typically store their cryptocurrency in digital "wallets," which are identified by unique electronic "addresses."

5. Each cryptocurrency transaction is recorded on a public ledger commonly referred to as a "blockchain," which acts as a public accounting record. The blockchain records, among other things, the date and time of each cryptocurrency transaction, the unique cryptocurrency addresses associated with the transaction, and the amount of cryptocurrency transferred. Like

cryptocurrencies, there are multiple types of blockchains.

6. "Blocks" are data structures within a blockchain database where transaction information is permanently recorded. They are the fundamental building blocks of the blockchain.

The Ethereum Network

7. The conduct described herein relates to the Ethereum Network. Among other things, Ethereum is a decentralized blockchain that is used by millions of people across the world. Since at least 2023, on average, there are more than one million daily transactions on the Ethereum blockchain. No central actor runs the Ethereum Network. Instead, the Ethereum Network is run through a decentralized network of participants across the world that operate based on a set of rules and protocols. These rules and protocols are typically executed through "smart contracts"—self-executing computer protocols with if/then conditions—which enable transactions to take place on the Ethereum blockchain without the need for a trusted intermediary. Ether or "ETH" is the native cryptocurrency on the Ethereum Network.

8. "Validators" are a critical participant in the Ethereum Network. Validators are responsible for checking that new blocks are valid before they are added to the Ethereum blockchain. Accordingly, the validation process is essential to ensuring the integrity and security of the Ethereum blockchain. To become a validator, the validator must "stake," or deposit, 32 ETH in a smart contract. Ethereum randomly selects a validator to validate a block; once selected, a validator has approximately 12 seconds to complete the validation process. For validating a new block on the Ethereum blockchain, a validator is paid an agreed-upon amount of cryptocurrency that represents a particular portion of the maximum extractable value (described below) of the transactions that comprise the new block and other fees, including validator tips. In addition, a validator earns cryptocurrency in the form of newly-minted ETH. If a validator attempts to defraud

the Ethereum blockchain or otherwise improperly performs their validator duties, the staked ETH in their smart contract can be "slashed" or cut.

9. When a user conducts a transaction on the Ethereum blockchain, such as a buy or sell trade, this transaction is not immediately added to the blockchain. Instead, the pending transaction waits alongside other pending transactions in the "memory pool" or "mempool," which is publicly visible. It is only after, among other things, pending transactions are structured into a proposed block, which is then validated by a validator, that pending transactions are added to the blockchain. After a block is published to the blockchain, the block is closed and cannot be altered or removed.

Maximal Extractable Value, Searchers, Builders, and Relays

10. Pending transactions in the mempool are not processed in chronological order, but rather according to their potential "maximal extractable value" or "MEV." MEV is the maximum value that can be obtained by including, reordering, or excluding transactions when publishing a new block to the blockchain. Without coordinated block-building protocols, competition among validators for MEV opportunities often causes network congestion and instability.

11. "MEV-Boost" is an open-source software designed to optimize the block-building process for Ethereum validators by establishing protocols for how transactions are organized into blocks. Approximately 90% of Ethereum validators use MEV-Boost.

12. Using MEV-Boost, Ethereum validators outsource the block-building process to a network of "searchers," "builders," and "relays." These participants operate pursuant to privacy and commitment protocols designed to ensure that each network participant—the searcher, the builder, and the validator—interacts in an ordered manner that maximizes value and network efficiency.

13. A searcher is effectively a trader who scans the public mempool for profitable arbitrage opportunities using automated bots ("MEV Bots"). After identifying a profitable opportunity (that would, for example, increase the price of a given cryptocurrency), the searcher sends the builder a proposed "bundle" of transactions. The bundle typically consists of the following transactions in a precise order: (a) the searcher's "frontrun" transaction, in which the searcher purchases some amount of cryptocurrency whose value the searcher expects to increase; (b) the pending transaction in the mempool that the MEV Bot identified would increase the price of that cryptocurrency; and (c) the searcher's sell transaction, in which the searcher sells the cryptocurrency at a higher price than what the searcher initially paid in order to extract a trading profit. A builder receives bundles from various searchers and compiles them into a proposed block that maximizes MEV for the validator. The builder then sends the proposed block to a "relay." A relay receives the proposed block from the builder and initially only submits the "blockheader" to the validator, which contains information about, among other things, the payment the validator will receive for validating the proposed block *as structured by the builder*. It is only *after* the validator makes this commitment through a digital signature that the relay releases the full content of the proposed block (*i.e.* – the complete ordered transaction list) to the validator.

14. In this process, a relay acts in a manner similar to an escrow account, which temporarily maintains the otherwise private transaction data of the proposed block until the validator commits to publishing the block to the blockchain exactly as ordered. The relay will not release the transactions within the proposed block to the validator until the validator has confirmed through a digital signature that it will publish the proposed block as structured by the builder to the blockchain. Until the transactions within the proposed block are released to the validator, they remain private and are not publicly visible.

15. Tampering with these established MEV-Boost protocols, which are relied upon by the vast majority of Ethereum users, threatens the stability and integrity of the Ethereum blockchain for all network participants.

The Exploit

16. Over the course of several months, ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO, the defendants, carefully planned and executed the Exploit, which was carried out through the use of at least one computer, and laid the groundwork to launder the proceeds from the Exploit. Indeed, as explained below, as early as in or about December 2022, ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO created and shared with each other online a document setting forth their plans for the Exploit.

17. ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO took the following steps, among others, to plan and execute the Exploit: (a) establishing a series of Ethereum validators in a manner that concealed their identities through the use of shell companies, intermediary cryptocurrency addresses, foreign exchanges, and a privacy layer network; (b) deploying a series of test transactions or "bait transactions" designed to identify particular variables most likely to attract MEV Bots that would become the victims of the Exploit (collectively the "Victim Traders"); (c) identifying and exploiting a vulnerability in the MEV-Boost relay code that caused the relay to prematurely release the full content of a proposed block; (d) re-ordering the proposed block to the defendants' advantage; and (e) publishing the re-ordered

block to the Ethereum blockchain, which resulted in the theft of approximately $25 million in cryptocurrency from the Victim Traders.

Establishing Ethereum Validators

18. In late December 2022, and in furtherance of their Exploit plan, ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO, the defendants established a company, Pine Needle Inc. ("Pine Needle"). On company registration documents, ANTON PERAIRE-BUENO is listed as Pine Needle's president and JAMES-PERAIRE BUENO is listed as its treasurer. On or about January 4, 2023, ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO opened a bank account (the "Pine Needle Bank-1 Account") at a bank ("Bank-1"). The Pine Needle Bank-1 Account was funded in part by deposits from personal bank accounts the defendants opened in January 2023 at another bank ("Bank-2"). In February 2023, ANTON PERAIRE-BUENO opened an account with a centralized cryptocurrency exchange (the "Pine Needle Exchange Account"), which the defendants funded with deposits from the Pine Needle Bank-1 Account.

19. Around the same time that ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO, the defendants, were opening bank and cryptocurrency accounts for Pine Needle, ANTON PERAIRE-BUENO, the defendant, searched online for cryptocurrency exchanges with limited "know your customer" protocols and ways to launder cryptocurrency, including searches for "how to wash crypto" and "cefi exchanges with no kyc." Then, between on or about February 28, 2023 and on or about March 20, 2023, the Pine Needle Exchange Account sent approximately 529.5 ETH to approximately 14 intermediary addresses, either directly or indirectly, through a foreign-based cryptocurrency exchange. During the same period, these intermediary addresses sent the identical amount of cryptocurrency to a privacy layer network on the Ethereum blockchain, which enables users, among other things, to conceal information concerning their

identity and source of funds on the blockchain. This approximately 529.5 ETH (then-worth approximately $880,000) was used thereafter to create 16 Ethereum validators (the "Validators") that were used to execute the Exploit, as explained below.

Baiting the Victim Traders and Identifying a Vulnerability in the Relay

20. On or about December 12, 2022, ANTON PERAIRE-BUENO, the defendant, visited a particular website ("Website-1") that hosted the open source code for MEV-Boost relay (the "Relay"), which, as discussed below, was impaired in a manner that compromised the integrity of the Relay code during the Exploit. Later that same month, ANTON PERAIRE-BUENO ran online searches related to Ethereum validator penalties for misconduct—a foreseen consequence of carrying out the Exploit.

21. On or about December 27, 2022, ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO, the defendants, created and shared a document (the "Exploit Plan"), which outlined a four-step plan to successfully execute the Exploit. In particular, the defendants identified four stages—"1. The Bait," "2. Unblinding the Block," "3. The Search," and "4. The Propagation." In the months that followed, the defendants followed each stage as outlined in their Exploit Plan.

22. With respect to the "bait," ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO, the defendants, targeted three Victim Traders ("Victim Trader-1," "Victim Trader-2," and "Victim Trader-3,"), who are searchers who operate MEV Bots that specialize in cryptocurrency arbitrage trading. In the "bait" phase, the defendants tested a series of bait transactions, which the MEV Bots operated by the Victim Traders identified as presenting a lucrative arbitrage opportunity that caused the Victim Traders to propose bundles to the builder

that included the bait transactions. In so doing, the defendants learned the trading behaviors of the Victim Trader's MEV Bots.

Carrying Out the Exploit

23. On or about April 2, 2023, ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO, the defendants, carried out the Exploit, through which they stole approximately $25 million worth of cryptocurrency from the Victim Traders.

24. First, after receiving notification that one of their 16 Validators had been selected to validate a new block, ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO, the defendants, lured the Victim Traders' MEV Bots by proposing at least eight specific transactions (the "Lure Transactions") that, based on the bait transactions described above, the defendants knew would cause the Victim Traders' MEV Bots to propose bundles that included the Lure Transactions. The Lure Transactions did, in fact, cause the Victim Traders to propose approximately eight bundles that included the Lure Transactions, which were submitted to the builder. In each of these eight bundles, the Victim Traders effectively bought substantial amounts of particularly illiquid cryptocurrencies (the frontrun trades), whose price the Victim Traders expected to increase as a result of the Lure Transactions, for approximately $25 million of various stablecoins, whose value is pegged to the U.S. dollar, or other more liquid cryptocurrencies. The Victim Traders also included a sell transaction in each bundle, whereby the Victim Traders would sell their newly acquired cryptocurrency—immediately after the Lure Transaction—at a higher price than what they bought it for. Importantly, the Victim Traders' bundles included coded conditions that the frontrun trades would not be executed unless: (a) the Lure Transactions took place immediately after the frontrun trades; *and* (b) the sell transactions took place immediately

after the Lure Transactions. The builders, in turn, submitted the proposed block with the ordered transaction bundles to the Relay.

25. Second, having timed the Lure Transactions to coincide to a period where one of their 16 Validators was selected to validate the proposed block, ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO, the defendants, used one of the Validators (the "Malicious Validator") to validate—and tamper with—the proposed block containing the Victim Traders' ordered transactions, which the block builder had privately submitted to the Relay.

26. Third, after the Relay released the blockheader for the proposed block which contained the Victim Traders' ordered transactions, ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO, the defendants, exploited a vulnerability in the Relay's computer code by sending the Relay a false signature (the "False Signature") in lieu of a valid digital signature. Based on their research and planning prior to the Exploit, ANTON PERAIRE-BUENO and JAMES PERAIRE-BUENO knew that the information contained in the False Signature could not be verified for ultimate publication to the blockchain. Instead, this False Signature was designed to, and did, trick the Relay to prematurely release the full content of the proposed block to the defendants, including the private transaction information. Once in possession of the Victim Traders' ordered transactions, the defendants tampered with the proposed block in the following manner:

a. The defendants allowed the Victim Traders to complete their buy transactions (*i.e.*, their frontrun trades). In effect, the Victim Traders sold approximately $25 million of various stablecoins or other more liquid cryptocurrencies to purchase particularly illiquid cryptocurrencies.

b. Defying the protocols of the Relay and the MEV-Boost system generally,